BostonSolux™
FOCUS ON SOLUTIONS

PECB

PECB CERTIFIED ISO/IEC 27032
Lead Cybersecurity Manager

Maîtriser la mise en œuvre et le management d'un programme de cybersécurité basé sur la norme ISO/IEC 27032

Pourquoi devriez-vous y participer ?

La formation ISO/CEI 27032 Lead Cybersecurity Manager vous permettra de développer les connaissances et les compétences nécessaires pour accompagner une organisation dans la mise en œuvre et la gestion d'un programme de cybersécurité en conformité avec la norme ISO/CEI 27032 et le Cadre de Cybersécurité NIST. Cette formation est conçue de manière à vous doter de connaissances approfondies en matière de cybersécurité, et vous permettra de maîtriser la relation entre la cybersécurité et d'autres types de sécurité des technologies de l'information, ainsi que le rôle des parties prenantes dans la cybersécurité.

Après avoir maîtrisé l'ensemble des concepts relatifs à la cybersécurité, vous pouvez vous présenter à l'examen et postuler au titre de « PECB Certified ISO/CEI 27032 Lead Cybersecurity Manager ». En étant titulaire d'une certification de PECB, vous démontrerez que vous disposez des connaissances pratiques et des compétences professionnelles pour soutenir et diriger une équipe dans la gestion de la cybersécurité.

À qui s'adresse la formation ?

- Professionnels de la cybersécurité
- Experts en sécurité de l'information
- Professionnels souhaitant gérer un programme de cybersécurité
- Responsables du développement d'un programme de cybersécurité
- Spécialistes des TI
- Conseillers spécialisés dans les TI
- Professionnels des TI souhaitant accroître leurs connaissances et compétences techniques

Programme de la formation

Durée : 5 jours

Jour 1 | Introduction à la cybersécurité et aux notions connexes, selon la recommandation de la norme ISO/IEC 27032

- Objectifs et structure du cours
- Normes et cadres réglementaires
- Notions fondamentales de la cybersécurité
- Programme de cybersécurité
- Lancer un programme de cybersécurité
- Analyser l'organisme
- Leadership

Jour 2 | Politiques de cybersécurité, management du risque et mécanismes d'attaque

- Politiques de cybersécurité
- Gestion du risque de la cybersécurité
- Mécanismes d'attaque

Jour 3 | Mesures de contrôle de cybersécurité, partage et coordination de l'information

- Mesures de contrôle de cybersécurité
- Partage et coordination de l'information
- Programme de formation et de sensibilisation

Jour 4 | Gestion des incidents, suivi et amélioration continue

- Continuité des activités
- Management des incidents de cybersécurité
- Intervention et récupération en cas d'incident de cybersécurité
- Conclusion de la formation
- Tests en cybersécurité
- Mesure de la performance
- Amélioration continue

Jour 5 | Examen de certification

Objectifs d'apprentissage

- Acquérir des connaissances approfondies sur les composantes et les opérations d'un programme de cybersécurité en conformité avec l'ISO/IEC 27032 et le cadre de cybersécurité NIST
- Comprendre la corrélation entre ISO 27032, le cadre de cybersécurité NIST et les autres normes et cadres réglementaires
- Maîtriser les concepts, approches, normes, méthodes et techniques pour établir, mettre en œuvre et gérer efficacement un programme de cybersécurité au sein d'un organisme
- Apprendre à interpréter les exigences d'ISO/IEC 27032 dans le contexte spécifique d'un organisme
- Maîtriser l'expertise nécessaire pour planifier, mettre en œuvre, gérer, contrôler et maintenir un programme de cybersécurité tel que spécifié dans ISO/IEC 27032 et le cadre de cybersécurité NIST
- Acquérir les compétences pour conseiller un organisme sur les bonnes pratiques de management de la cybersécurité

Examen

Durée : 3 heures

L'examen « PECB Certified ISO/CEI 27032 Lead Cybersecurity Manager » remplit les exigences relatives au programme d'examen et de certification de PECB. L'examen couvre les domaines de compétences suivants :

Domaine 1 | Principes et concepts fondamentaux de la cybersécurité

Domaine 2 | Rôles et responsabilités des parties prenantes

Domaine 3 | Gestion des risques liés à la cybersécurité

Domaine 4 | Mécanismes d'attaque et contrôles en cybersécurité

Domaine 5 | Partage de l'information et coordination

Domaine 6 | Intégrer le programme de cybersécurité dans le management de la continuité des activités

Domaine 7 | Gestion des incidents de cybersécurité et mesure de la performance.

Pour de plus amples informations concernant l'examen, veuillez consulter Politiques et règlement relatifs à l'examen

Certification

Après avoir réussi l'examen, vous pouvez demander l'une des qualifications mentionnées sur le tableau ci-dessous. Un certificat vous sera délivré si vous remplissez toutes les exigences relatives à la qualification sélectionnée.

Pour de plus amples informations concernant les certifications ISO/CEI 27032 et le processus de certification PECB, veuillez cliquer sur Politiques et règlement de certification.

Qualification	Examen	Expérience professionnelle	Expérience de projets en cybersécurité	Autres exigences
PECB Certified ISO/IEC 27032 Provisional Cybersecurity Manager	Examen PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager ou équivalent	Aucune	Aucune	Signer le Code de déontologie de PECB
PECB Certified ISO/IEC 27032 Cybersecurity Manager	Examen PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager ou équivalent	2 ans dont 1 an d'expérience en cyberséacurité	Activités de cybersécurité totalisant 200 heures	Signer le Code de déontologie de PECB
PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager	Examen PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager ou équivalent	5 ans dont 2 ans d'expérience en cybersécurité	Activités de cybersécurité totalisant 300 heures	Signer le Code de déontologie de PECB
PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager	Examen PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager ou équivalent	10 ans dont 7 ans d'expérience en cybersécurité	Activités de cybersécurité totalisant 1 000 heures	Signer le Code de déontologie de PECB

Note : *Les personnes certifiées par PECB qui possèdent les certifications Lead Cybersecurity Manager et Lead Incident Manager sont qualifiées pour la certification* ***Master Cybersecurity de PECB****, étant donné qu'elles ont passé 4 examens de base supplémentaires liés à ce programme. Pour des informations plus détaillées sur les examens de base et les exigences générales du Master, veuillez visiter le lien suivant : https://pecb.com/en/master-credentials*

Informations générales

- Les frais de certification sont inclus dans le prix de l'examen
- Un manuel de cours contenant plus de 400 pages d'informations et d'exemples pratiques est fourni
- À l'issue de la formation, un certificat de participation de 31 crédits DPC (Développement professionnel continu) est délivré
- En cas d'échec à l'examen, vous pouvez le repasser dans les 12 mois qui suivent sans frais supplémentaires

BostonSolux™
FOCUS ON SOLUTIONS

PECB

PECB Certified ISO/IEC 27005
Risk Manager

Maîtrisez les principes et les concepts fondamentaux de l'appréciation des risques et de la gestion optimale des risques liés à la sécurité de l'information conformément à la norme ISO/IEC 27005

Pourquoi devriez-vous y participer ?

La formation « ISO/IEC 27005 Risk Manager » vous permettra de développer les compétences nécessaires pour maîtriser les processus liés à tous les actifs pertinents pour la sécurité de l'information en utilisant la norme ISO/IEC 27005 comme cadre de référence. Au cours de cette formation, nous présenterons également d'autres méthodes d'appréciation des risques telles qu'OCTAVE, EBIOS, MEHARI et la méthodologie harmonisée EMR. Cette formation s'inscrit parfaitement dans le processus de mise en œuvre du cadre SMSI selon la norme ISO/IEC 27001.

Après avoir compris l'ensemble des concepts relatifs à la gestion des risques de la sécurité d'information conformément à la norme ISO/IEC 27005 et réussi l'examen, vous pourrez demander la certification « ISO/IEC 27005 Risk Manager ». Détenir une certification PECB vous permettra de démontrer que vous disposez des connaissances et des compétences nécessaires pour réaliser une appréciation optimale des risques de la sécurité de l'information et pour gérer les risques de la sécurité de l'information dans les délais.

À qui s'adresse la formation ?

- Responsables de la sécurité d'information
- Membres d'une équipe de sécurité de l'information
- Tout individu responsable de la sécurité d'information, de la conformité et du risque dans une organisation
- Tout individu mettant en œuvre ISO/IEC 27001, désirant se conformer à la norme ISO/IEC 27001 ou impliqué dans un programme de gestion des risques
- Consultants des TI
- Professionnels des TI
- Agents de la sécurité de l'information
- Agents de la protection des données personnelles

Programme de la formation

Durée : 3 jours

Jour 1 | Introduction au programme de gestion des risques conforme à ISO/IEC 27005

- Objectifs et structure de la formation
- Cadres normatifs et règlementaires
- Concepts et définitions du risque
- Programme de gestion des risques
- Établissement du contexte

Jour 2 | Mise en œuvre d'un processus de gestion des risques conforme à ISO/IEC 27005

- Identification des risques
- Analyse et évaluation des risques
- Appréciation du risque avec une méthode quantitative
- Traitement des risques
- Acceptation des risques et gestion des risques résiduels
- Communication relative aux risques
- Surveillance et réexamen des risques

Jour 3 | Aperçu des autres méthodes d'appréciation des risques liés à la sécurité de l'information et examen de certification

- Méthode OCTAVE
- Méthode MEHARI
- Méthode EBIOS
- Méthodologie harmonisée d'EMR
- Clôture de la formation

Objectifs de la formation

- Comprendre la relation entre la gestion des risques de la sécurité de l'information et les mesures de sécurité
- Comprendre les concepts, approches, méthodes et techniques permettant un processus de gestion des risques efficace et conforme à ISO/IEC 27005
- Savoir interpréter les exigences de la norme ISO/IEC 27001 dans le cadre de la gestion des risques de la sécurité de l'information
- Acquérir les compétences pour conseiller efficacement les organisations sur les meilleures pratiques en matière de gestion des risques liés à la sécurité de l'information

Examen

Durée : 2 heures

L'examen « PECB Certified ISO/IEC 27005 Risk Manager » remplit les exigences relatives au programme d'examen et de certification de PECB. L'examen couvre les domaines de compétences suivants :

Domaine 1 | Principes et concepts fondamentaux relatifs à la gestion des risques liés à la sécurité de l'information

Domaine 2 | Mettre en œuvre un programme de gestion des risques liés à la sécurité de l'information

Domaine 3 | Processus et cadre de gestion des risques liés à la sécurité de l'information conformes à la norme ISO/IEC 27005

Domaine 4 | Autres méthodes d'appréciation des risques de la sécurité de l'information

Pour de plus amples informations concernant l'examen, veuillez consulter les Politiques et règlement relatifs à l'examen

Certification

Après avoir réussi l'examen, vous pouvez demander l'un des qualifications mentionnées sur le tableau ci-dessous. Un certificat vous sera délivré si vous remplissez toutes les exigences relatives à la qualification sélectionnée

Pour de plus amples informations concernant les certifications ISO/IEC 27005 et le processus de certification PECB, veuillez cliquer sur les Politiques et règlement de certification

Qualification	Examen	Expérience professionnelle	Expérience en management du risque	Autres exigences
PECB Certified ISO/IEC 27005 Provisional Risk Manager	Examen « PECB Certified ISO/IEC 27005 Risk Manager » ou équivalent	Aucune	Aucune	Signer le Code de déontologie de PECB
PECB Certified ISO/IEC 27005 Risk Manager	Examen « PECB Certified ISO/IEC 27005 Risk Manager » ou équivalent	Deux ans, dont un an d'expérience en gestion des risques	Activités de gestion des risques totalisant 200 heures	Signer le Code de déontologie de PECB

Informations générales

- Les frais de certification sont inclus dans le prix de l'examen.
- Un manuel de cours contenant plus de 350 pages d'informations et d'exemples pratiques est fourni.
- À l'issue de la formation, un certificat de présence de 21 crédits FPC (Formation professionnelle continue) est délivré.
- En cas d'échec à l'examen, vous pouvez le reprendre sans frais dans les 12 mois suivants.

BostonSolux™
FOCUS ON SOLUTIONS

PECB

PECB Certified ISO/CEI 27001
Lead Auditor

Maîtriser l'audit des systèmes de management de la sécurité de l'information (SMSI) conformément à la norme ISO/IEC 27001:2022

Pourquoi devriez-vous y participer ?

Les menaces et les attaques contre la sécurité de l'information augmentent et évoluent sans cesse. Les organismes sont donc de plus en plus préoccupés par la manière dont leurs précieuses informations sont traitées et protégées. La meilleure forme de défense contre les menaces et les attaques est la mise en œuvre, l'audit et le management appropriés des mesures de sécurité de l'information et des bonnes pratiques. La sécurité de l'information est une attente et une exigence essentielle des clients, des législateurs et des autres parties intéressées.

La formation PECB ISO/IEC 27001 Lead Auditor est conçue pour vous préparer à diriger l'audit d'un système de management de la sécurité de l'information (SMSI) basé sur la norme ISO/IEC 27001. Au cours de cette formation, vous acquerrez les connaissances et les compétences nécessaires pour planifier et réaliser des audits internes et externes conformément aux processus de certification des normes ISO 19011 et ISO/IEC 17021-1.

La formation comprend des exercices pratiques et des études de cas qui vous apportent une expertise concrète que vous pouvez appliquer à vos opérations et activités quotidiennes. Grâce aux exercices pratiques, vous maîtriserez les techniques d'audit et deviendrez compétent pour gérer un programme d'audit, une équipe d'audit, la communication avec les clients et pour résoudre les conflits.

Nos formations sont exhaustives, ce qui signifie qu'elles couvrent tout ce dont vous avez besoin pour obtenir la certification. Après avoir acquis les compétences nécessaires pour réaliser un audit, vous pourrez passer l'examen et demander la certification « PECB Certified ISO/IEC 27001 Lead Auditor ». En obtenant un certificat PECB Lead Auditor, vous pourrez démontrer que vous disposez des capacités et des compétences nécessaires pour auditer des organisations conformément aux bonnes pratiques.

Pourquoi cette formation est-elle préférable aux autres ?

La formation PECB Certified ISO/IEC 27001 Lead Auditor est précieuse et préférable aux autres en ce qu'elle vous donne les connaissances et les compétences nécessaires pour diriger l'audit d'un système de management de la sécurité de l'information (SMSI). Par ailleurs, la formation vous apprend à appliquer ces compétences dans la pratique.

Outre la présentation de ce que la norme ISO/IEC 27001 vous demande de faire, cette formation vous enseigne comment le faire, à travers divers exercices, activités, études de cas, quiz autonomes à choix multiple et quiz basés sur des scénarios. Ceux-ci vous permettront de tester vos connaissances sur les étapes du processus d'audit.

Après avoir acquis l'expertise nécessaire pour effectuer cet audit, vous pouvez vous présenter à l'examen et demander le titre de « PECB Certified ISO/IEC 27001 Lead Auditor ». En détenant un certificat PECB Lead Auditor, vous serez en mesure de démontrer que vous disposez des capacités et des compétences nécessaires pour auditer des organisations conformément aux bonnes pratiques.

Qu'est-ce que la certification vous permettra de faire ?

La certification est la reconnaissance formelle et la preuve de connaissances qui ont une valeur considérable lorsque vous entrez sur le marché du travail ou lorsque vous voulez avancer dans votre carrière. En raison des progrès technologiques et de la complexité des cyberattaques, la demande de professionnels de la sécurité de l'information ne cesse de croître. À ce titre, la certification ISO/IEC 27001 est devenue la norme en matière de bonnes pratiques d'audit de la sécurité de l'information. En obtenant une certification, vous mettez en évidence un certain niveau de compétences qui apportera une valeur ajoutée non seulement à votre carrière professionnelle, mais aussi à votre société. Elle peut vous aider à vous démarquer et à augmenter votre potentiel de gain.

À qui s'adresse la formation ?

- Auditeurs souhaitant effectuer et diriger des audits de certification du système de management de sécurité de l'information (SMSI)
- Managers ou consultants souhaitant maîtriser le processus d'audit d'un système de management de sécurité de l'information
- Personnes responsables de maintenir la conformité aux exigences du système de management de sécurité de l'information.
- Experts techniques souhaitant se préparer à un audit du système de management de sécurité de l'information.
- Conseillers experts en management de sécurité de l'information

Programme de la formation

Durée : 5 jours

Jour 1 | Introduction au système de management de la sécurité de l'information (SMSI) et à ISO/IEC 27001

- Objectifs et structure de la formation
- Normes et cadres réglementaires
- Processus de certification
- Concepts et principes fondamentaux de la sécurité de l'information
- Système de management de la sécurité de l'information (SMSI)

Jour 2 | Principes d'audit, préparation et initiation d'un audit

- Concepts et principes fondamentaux de l'audit
- Impact des tendances et de la technologie sur l'audit
- Audit fondé sur des preuves
- Audit fondé sur le risque
- Initiation du processus d'audit
- Étape 1 de l'audit

Jour 3 | Activités d'audit sur site

- Préparation à l'étape 2 de l'audit
- Étape 2 de l'audit
- Communication durant l'audit
- Procédures d'audit
- Création de plans de test d'audit

Jour 4 | Clôture de l'audit

- Rédaction des constatations d'audit et des rapports de non-conformité
- Documentation d'audit et revue de qualité
- Clôture de l'audit
- Évaluation des plans d'action par l'auditeur
- Après l'audit initial
- Management d'un programme d'audit interne
- Clôture de la formation

Jour 5 | Examen de certification

Objectifs de la formation

À l'issue de cette formation, les participants seront capables de :

- Expliquer les concepts et les principes fondamentaux d'un système de management de la sécurité de l'information (SMSI) basé sur ISO 27001
- Interpréter les exigences d'ISO 27001 pour un SMSI du point de vue d'un auditeur
- Évaluer la conformité du SMSI aux exigences d'ISO 27001, en accord avec les concepts et les principes fondamentaux d'audit
- Planifier, réaliser et clôturer un audit de conformité à ISO 27001, conformément aux exigences d'ISO/IEC 17021-1, aux lignes directrices d'ISO 19011 et aux autres bonnes pratiques d'audit
- Gérer un programme d'audit ISO/IEC 27001

Examen

Durée : 3 heures

L'examen « PECB Certified ISO/IEC 27001 Lead Auditor » répond pleinement aux exigences du Programme d'examen et de certification PECB (PEC). L'examen couvre les domaines de compétences suivants :

Domaine 1 | Principes et concepts fondamentaux d'un système de management de sécurité de l'information (SMSI)

Domaine 2 | Système de management de la sécurité de l'information (SMSI)

Domaine 3 | Concepts et principes fondamentaux de l'audit

Domaine 4 | Préparation d'un audit ISO/IEC 27001

Domaine 5 | Réalisation d'un audit ISO/IEC 27001

Domaine 6 | Clôture d'un audit ISO/IEC 27001

Domaine 7 | Gestion d'un programme d'audit ISO/IEC 27001

Pour plus d'informations sur les détails de l'examen, veuillez consulter les Politiques et règlement relatifs à l'examen

Certification

Après avoir réussi l'examen, vous pouvez demander l'une des certifications mentionnées dans le tableau ci-dessous. Un certificat vous sera délivré si vous remplissez toutes les exigences relatives à la certification sélectionnée.

Pour plus d'informations sur les certifications IEC 27001 et le processus de certification PECB, veuillez consulter les Règles et politiques relatives à la certification

Titre de compétence	Examen	Expérience professionnelle	Expérience d'audit/évaluation du SM	Autres exigences
PECB Certified ISO/IEC 27001 Provisional Auditor	Examen PECB Certified ISO/IEC 27001 Lead Auditor ou équivalent	Aucune	Aucune	Signer le Code de déontologie de PECB
PECB Certified ISO/IEC 27001 Auditor	Examen PECB Certified ISO/IEC 27001 Lead Auditor ou équivalent	**Deux ans,** dont 1 an d'expérience en management de la sécurité de l'information	200 heures	Signer le Code de déontologie de PECB
PECB Certified ISO/IEC 27001 Lead Auditor	Examen PECB Certified ISO/IEC 27001 Lead Auditor ou équivalent	**Cinq ans,** dont 2 ans d'expérience en management de la sécurité de l'information	300 heures	Signer le Code de déontologie de PECB
PECB Certified ISO/IEC 27001 Senior Lead Auditor	Examen PECB Certified ISO/IEC 27001 Lead Auditor ou équivalent	**Dix ans,** dont 7 ans d'expérience en management de la sécurité de l'information	1,000 heures	Signer le Code de déontologie de PECB

Remarque :*Les personnes certifiées PECB qui possèdent à la fois les titres de Lead Implementer et Lead Auditor sont qualifiées pour la certification* ***PECB Master****, à condition qu'elles aient passé quatre examens Foundation supplémentaires liés à ce programme. Pour plus d'informations sur les examens Foundation et les exigences générales relatives au Master, reportez-vous au lien suivant : https://pecb.com/en/master-credentials.*

Informations générales

- Les frais d'examen et de certification sont inclus dans le prix de la session de formation.
- PECB fournira un manuel de formation contenant plus de 450 pages d'informations et d'exemples pratiques.
- Une Attestation d'achèvement de formation de 31 unités de FPC (Formation professionnelle continue) sera délivrée aux participants ayant suivi la formation.
- En cas d'échec à l'examen, le candidat peut le reprendre une fois gratuitement dans les 12 mois suivant la date de l'examen initial.

BostonSolux™
FOCUS ON SOLUTIONS

PECB

PECB Certified ISO/IEC 27001
Lead Implementer

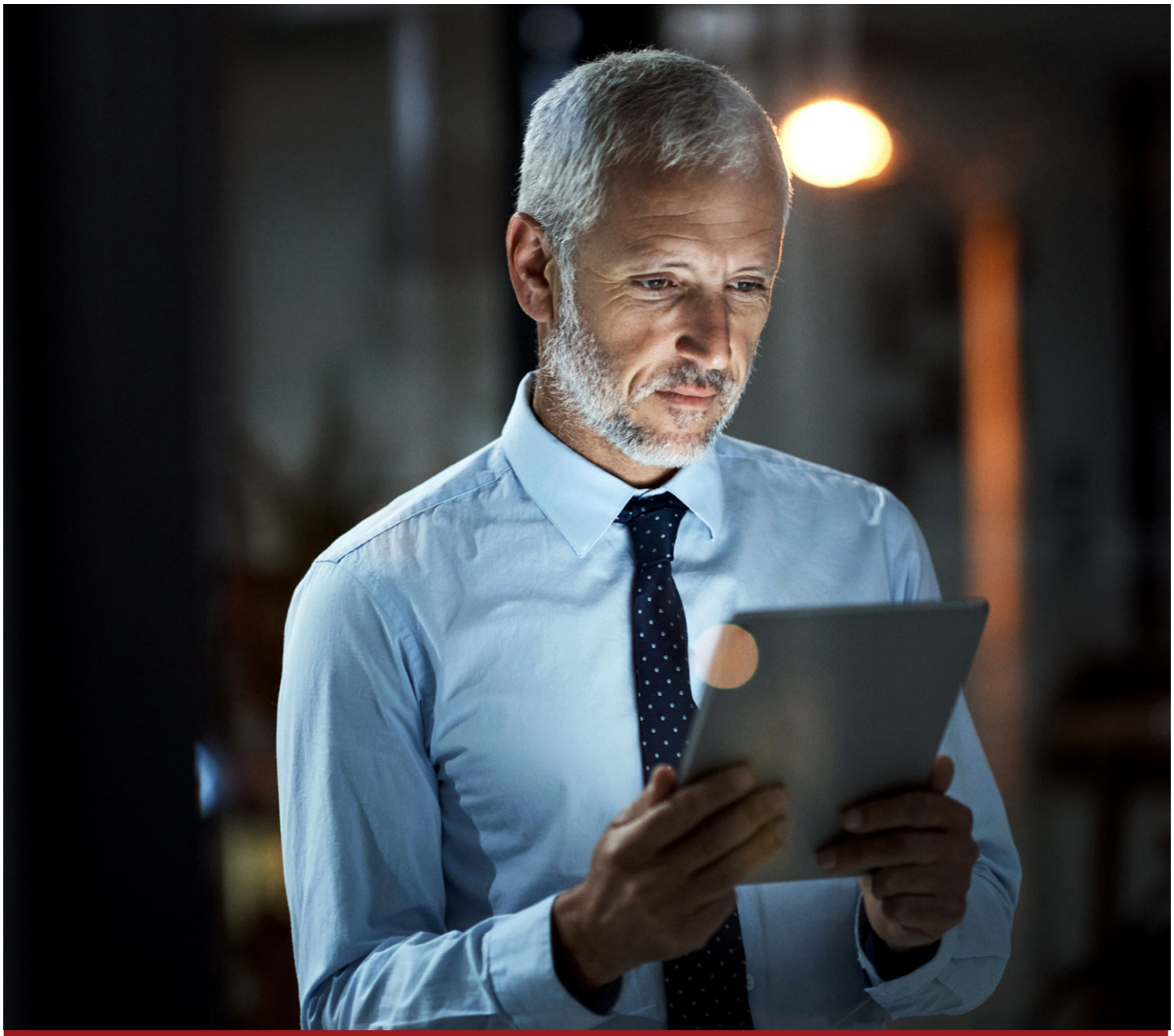
Maîtrisez la mise en œuvre et la gestion d'un Système de management de la sécurité de l'information (SMSI) conforme à la norme ISO/CEI 27001:2022

Pourquoi devriez-vous y participer à cette formation ?

Les menaces et les attaques contre la sécurité de l'information augmentent et s'améliorent constamment. La meilleure forme de défense contre elles est la mise en œuvre et le management appropriés des mesures et des bonnes pratiques en matière de sécurité de l'information. La sécurité de l'information est également une attente et une exigence essentielle des clients, des législateurs et des autres parties intéressées.

Cette formation est conçue pour préparer les participants à la mise en œuvre d'un système de management de la sécurité de l'information (SMSI) basé sur la norme ISO/IEC 27001. Elle vise à fournir une compréhension complète des bonnes pratiques d'un SMSI et un cadre pour sa gestion et son amélioration continues.

La formation comprend de nombreux exercices pratiques et études de cas qui vous permettront d'acquérir une expertise concrète que vous pourrez appliquer à vos opérations et activités quotidiennes. Nos formations sont exhaustives, ce qui signifie qu'elles couvrent tout ce dont vous avez besoin pour obtenir le certificat.



Pourquoi cette formation est-elle préférable aux autres ?

La formation PECB Certified ISO/IEC 27001 Lead Implementer est précieuse et préférable aux autres en ce qu'elle vous permet non seulement d'acquérir les connaissances et les compétences nécessaires à la mise en œuvre d'un système de management de la sécurité de l'information (SMSI), mais elle vous enseigne également comment appliquer les compétences requises dans la pratique. En plus de ce que la norme ISO/IEC 27001 vous dit de faire, cette formation vous enseigne comment le faire, à travers divers exercices, activités, études de cas, quiz autonomes à choix multiple et quiz basés sur des scénarios. Ceux-ci vous permettront de tester vos connaissances sur les étapes du processus de mise en œuvre.

Après avoir suivi cette formation, vous pouvez passer l'examen. Le type d'examen est unique, car il est à livre ouvert et contient des questions à choix multiples. Il contient également des questions indépendantes et des questions basées sur des scénarios, qui visent à simuler des situations de la vie réelle. Si vous le réussissez, vous pouvez demander le certificat PECB Certified ISO/IEC 27001 Lead Implementer, lequel démontre votre capacité et vos connaissances pratiques pour la mise en œuvre d'un SMSI basé sur les exigences d'ISO/IEC 27001.

Qu'est-ce que la certification vous permettra de faire ?

La certification est la reconnaissance formelle et la preuve de connaissances qui ont une valeur considérable lorsque vous entrez sur le marché du travail ou lorsque vous voulez avancer dans votre carrière. En raison des progrès technologiques et de la complexité des cyberattaques, la demande de professionnels IT reste élevée. À ce titre, la certification ISO/IEC 27001 est devenue la norme en matière de bonnes pratiques de sécurité de l'information. En passant une certification, vous mettez en avant un certain niveau de compétences qui apportera une valeur ajoutée non seulement à votre carrière professionnelle, mais aussi à votre société. Elle peut vous aider à vous démarquer et à augmenter votre potentiel de gain.

À qui s'adresse la formation ?

- Chefs de projet et consultants impliqués et concernés par la mise en œuvre d'un SMSI
- Conseillers experts cherchant à maîtriser la mise en œuvre d'un SMSI
- Personnes responsables d'assurer la conformité aux exigences de sécurité de l'information au sein d'une organisation.
- Membres d'une équipe de mise en œuvre d'un SMSI

Programme de la formation

Durée : 5 jours

Jour 1 | Introduction à la norme ISO/IEC 27001 et initiation d'un SMSI

- Objectifs et structure de la formation
- Normes et cadres réglementaires
- Système de management de la sécurité de l'information (SMSI)
- Concepts et principes fondamentaux de la sécurité de l'information
- Initiation de la mise en œuvre du SMSI
- Compréhension de l'organisation et de son contexte
- Périmètre du SMSI

Jour 2 | Planification de la mise en œuvre d'un SMSI

- Leadership et approbation du projet
- Structure organisationnelle
- Analyse du système existant
- Politique de sécurité de l'information
- Gestion des risques
- Déclaration d'applicabilité

Jour 3 | Mise en œuvre du SMSI

- Gestion des informations documentées
- Sélection et conception des mesures
- Mise en œuvre des mesures
- Tendances et technologies
- Communication
- Compétence et sensibilisation
- Gestion des opérations de sécurité

Jour 4 | Suivi, amélioration continue et préparation à l'audit de certification du SMSI

- Surveillance, mesure, analyse et évaluation
- Audit interne
- Revue de direction
- Traitement des non-conformités
- Amélioration continue
- Préparation à l'audit de certification
- Processus de certification et clôture de la formation

Jour 5 | Examen de certification

Objectifs de la formation

Cette formation vous aidera à :

- Acquérir une compréhension globale des concepts, approches, méthodes et techniques utilisés pour la mise en œuvre et la gestion efficace d'un SMSI
- Comprendre la corrélation entre ISO/IEC 27001, ISO/IEC 27002 ainsi qu'avec d'autres normes et cadres réglementaires
- Comprendre le fonctionnement d'un système de management de la sécurité de l'information et ses processus basés sur ISO/IEC 27001
- Apprendre à interpréter et à mettre en œuvre les exigences de la norme ISO 27001 dans le contexte spécifique d'un organisme
- Acquérir les connaissances nécessaires pour soutenir une organisation dans la planification, la mise en œuvre, la gestion, la surveillance et le maintien efficaces d'un SMSI

Examen

Durée : 3 heures

L'examen « PECB Certified ISO/IEC 27001 Lead Implementer » répond aux exigences du Programme d'examen et de certification PECB (PEC). L'examen couvre les domaines de compétence suivants :

Domaine 1 | Principes et concepts fondamentaux d'un système de management de la sécurité de l'information (SMSI)

Domaine 2 | Système de management de la sécurité de l'information (SMSI)

Domaine 3 | Planification de la mise en œuvre d'un SMSI selon ISO/IEC 27001

Domaine 4 | Mise en œuvre d'un SMSI selon ISO/IEC 27001

Domaine 5 | Surveillance et mesure d'un SMSI selon ISO/IEC 27001

Domaine 6 | Amélioration continue d'un SMSI selon ISO/IEC 27001

Domaine 7 | Préparation à un audit de certification du SMSI

Pour des informations spécifiques sur le type d'examen, les langues disponibles et d'autres détails, veuillez consulter la liste des examens PECB et les Politiques et règlement relatifs à l'examen.

Certification

Après avoir réussi l'examen, vous pouvez demander une des certifications présentées ci-dessous. Le certificat vous sera délivré si vous remplissez toutes les exigences relatives à la certification sélectionnée. Pour plus d'informations sur les certifications IEC 27001 et le processus de certification PECB, veuillez consulter les Règles et politiques relatives à la certification.

Titre de compétence	Examen	Expérience professionnelle	Expérience de projet SMSI	Autres exigences
PECB Certified ISO/IEC 27001 Provisional Implementer	Examen PECB Certified ISO/IEC 27001 Lead Implementer ou équivalent	Aucune	Aucune	Signer le Code de déontologie de PECB
PECB Certified ISO/IEC 27001 Implementer	Examen PECB Certified ISO/IEC 27001 Lead Implementer ou équivalent	**2 ans** (1 an en sécurité de l'information)	200 heures	Signer le Code de déontologie de PECB
PECB Certified ISO/IEC 27001 Lead Implementer	Examen PECB Certified ISO/IEC 27001 Lead Implementer ou équivalent	**5 ans** (2 ans en sécurité de l'information)	300 heures	Signer le Code de déontologie de PECB
PECB Certified ISO/IEC 27001 Senior Lead Implementer	Examen PECB Certified ISO/IEC 27001 Lead Implementer ou équivalent	**10 ans** (7 ans en sécurité de l'information)	1,000 heures	Signer le Code de déontologie de PECB

Remarque : *Les personnes certifiées par PECB qui possèdent les qualifications de Lead Implementer et Lead Auditor sont admissibles à l'obtention de la qualification Master de PECB, étant donné qu'elles ont passé 4 examens Foundation supplémentaires qui sont liés à ce programme. Pour en savoir plus sur les examens Foundation et les exigences générales de la qualification Master, veuillez consulter le lien suivant: https://pecb.com/en/master-credentials.*

Informations générales

- Les frais d'examen et de certification sont inclus avec la formation.
- Les participants recevront le matériel de formation contenant plus de 450 pages d'informations explicatives, d'exemples, de bonnes pratiques, d'exercices et de quiz.
- Une Attestation d'achèvement de formation de 31 unités de FPC (Formation professionnelle continue) sera délivrée aux participants ayant suivi la formation.
- En cas d'échec à l'examen, les candidats peuvent le repasser gratuitement dans les 12 mois suivant la tentative initiale.